RSA – Marche à suivre

Alice doit envoyer un message à Bob, elle a donc besoin de la clé publique RSA de Bob.

Voici les différentes étapes :

1) Bob choisit p et q deux grands nombres premiers (plus de 100 chiffres).
2) Bob calcule $n = p \cdot q$.

   Le nombre n, le modulo RSA, a environ 200 chiffres. Il est publique alors que p et q sont gardés secrets.
3) Bob calcule $\varphi(n) = (p-1)(q-1)$, à partir de la fonction d'Euler φ, et qui doit rester secret.

   Retrouver $\varphi(n)$ sans connaître p et q est aussi difficile que de factoriser n.
4) Bob choisit e en s'assurant que $\text{pgcd}(e, \varphi(n)) = 1$. Il s'agit de l'exposant RSA.
5) Bob calcule d, inverse de e modulo $\varphi(n)$ et garde secret le couple (n, d).

   Il s'agit de la clé privée RSA. Il la garde secrète afin de pouvoir décoder par la suite le message transmis par Alice.
6) Bob transmet (ou publie dans un annuaire) le couple (n, e). Ce couple s'appelle la clé publique RSA.
7) Alice convertit son message "texte" en un nombre (ou une suite de nombres) M compris entre 0 et n.
8) Alice calcule $\boxed{M' \equiv M^e \mod n}$ et envoie ce message chiffré M' à Bob.
9) Pour le déchiffrer, Bob calcule $\boxed{M \equiv M'^d \mod n}$ à l'aide de sa clé privée d.
   Cela lui permet de retrouver le message d'origine car :

$$M'^d \equiv (M^e)^d \equiv M^{ed} \equiv M \mod n$$

10) Finalement, Bob reconvertit ce nombre (ou ces nombres) en un message clair.